GTN-Québec

Groupe de travail québécois sur les normes et standards
en TI pour l'apprentissage, l'éducation et la formation

Publication 2011-05

Fédération d'identité pour les organismes de l'éducation

Recueil d'informations et identifications des principaux enjeux et des moyens de mise en œuvre

---

André Breton

Novembre 2011

Mission du GTN-Québec

La mission du Groupe de travail québécois sur les normes et standards pour l'apprentissage, l'éducation et la formation (GTN-Québec) est de fournir une expertise à la communauté éducative en matière de normalisation.

Les membres du GTN-Québec proviennent des trois ordres d'enseignement, des ministères, ainsi que du secteur privé de la formation. En s'appuyant sur les travaux des groupes internationaux d'élaboration des normes, ils soutiennent les acteurs du milieu de l'éducation pour favoriser l'implantation de pratiques communes de description et de production de ressources éducatives interopérables, réutilisables et accessibles à tous.

Ces ressources forment un patrimoine éducatif d'une valeur inestimable pour les communautés éducatives francophones. Assurer son enrichissement et sa pérennité est en conséquence, depuis sa fondation, au cœur des préoccupations du GTN-Québec.

Objectifs du GTN-Québec

1. Dans une perspective d'accompagnement, consulter les acteurs du milieu de l'éducation pour mieux définir comment les approches basées sur les normes et standards peuvent aider à concrétiser la mission éducative de leur organisation ;

2. Connaître des solutions basées sur des normes et standards, s'assurer qu'elles correspondent à la réalité et aux besoins du milieu et proposer, le cas échéant, des adaptations ou des guides d'utilisation de ces normes;

3. Faire connaître et encourager les pratiques normalisées de production et de description de ressources éducatives ;

4. Favoriser le développement d'une masse critique de REA numériques accessibles, pérennes et réutilisables au sein des établissements de chaque ordre d'enseignement ;

5. Maintenir l'expertise et la représentation québécoises en matière de développement de normes internationales et d'autres standards.

Les activités du GTN-Québec sont réalisées avec l'appui financier du ministère de l'Éducation, du Loisir et du Sport du Québec et grâce à la collaboration de ses membres.

www.gtn-quebec.org

ISBN 978-2-924168-13-4 (PDF)

Dépôt légal – Bibliothèque et Archives nationales du Québec, 2012
Dépôt légal – Bibliothèque et Archives Canada, 2012

Table des matières

Licence de la propriété intellectuelle

Cette étude a été réalisée avec le soutien financier du Groupe de travail québécois sur les normes et standards TI pour l'apprentissage, l'éducation et la formation (GTN-Québec). Le contenu de ce rapport demeure la responsabilité des auteurs. Les opinions qui y sont exprimées ne reflètent pas nécessairement celles du GTN-Québec.

GTN-Québec

La mission du Groupe de travail sur les normes du Québec (GTN-Québec) est de fournir une expertise en matière de normalisation en vue de promouvoir la création et l'enrichissement d'un patrimoine éducatif pour la communauté éducative.

Les membres du GTN-Québec proviennent des trois ordres d'enseignement, des ministères, ainsi que du secteur privé de la formation. En s'appuyant sur les travaux des groupes internationaux d'élaboration des normes, ils informent et soutiennent les acteurs du milieu de l'éducation pour favoriser l'implantation de pratiques normalisées de description et de production de ressources d'enseignement et d'apprentissage interopérables et réutilisables.

Les activités du GTN-Québec sont réalisées avec l'appui financier du ministère de l'Éducation du Loisir et du Sport du Québec et grâce à la contribution de ses membres.

Auteur

André Breton, ing. stag., a reçu son baccalauréat en 1996 de l'École Polytechnique de Montréal. Il poursuit présentement ses études en génie du logiciel pour l’obtention d’une maîtrise en ingénierie. Ses intérêts sont les processus de génie logiciel, les méthodes et outils de conception de logiciel, le contrôle et mesure de la qualité du logiciel, l’informatique mobile et la formation en ligne. Il travaille présentement comme analyste à la Société GRICS.

Sommaire

Face à l'émergence de fédérations d'identité dans le domaine de l'éducation dans plusieurs pays du monde, le GTN-Québec s'était donné le mandat de définir le concept de la fédération de l'identité dans le milieu scolaire québécois. L'objectif de cet article était de fournir les informations pertinentes et nécessaires aux organismes de l'éducation face à l'émergence d'une fédération d'identité. Ces informations devaient identifier et renseigner sur les enjeux et les moyens qui doivent être mis en œuvre dans la réalisation d'un tel projet. En consultant des intervenants des trois ordres d'enseignement et en définissant les principaux concepts et termes liés à la fédération d'identité, cet article amène les points saillants tant opérationnels que techniques. Du point de vue opérationnel, la fédération est présentée dans la perspective de sa gouvernance et techniquement, présentée avec les principaux services que l'on retrouve au sein des principales architectures rencontrées. Des listes non exhaustives concernant les politiques, les procédures, les risques et les étapes de mise en place sont aussi présentées. En conclusion, l'article retient la nature très actuelle et de l'importance de la gestion de l'identité dans un cadre des TIC dans plusieurs sphères d'activité et non seulement dans celle de l'éducation.

Introduction

Depuis l'arrivée du réseau Internet au sein des organismes scolaires, la gestion de l'identité numérique des membres représente un défi opérationnel, tactique et stratégique qui se complexifie continuellement au fil du temps. L'identité d'un individu varie en fonction du contexte. Ainsi, un individu voulant faire affaire avec le ministère du Revenu est identifié par son numéro d'assurance sociale et, dans le cas du ministère de l'Éducation, par son code permanent. Le même individu a probablement accès à différents portails, environnements numériques d'apprentissage, portfolios numériques, outils de gestion pédagogique, applications de gestion administrative, livres et éditions numériques, etc. Cette multiplication des services et des applications demande d'envisager l'ensemble de la problématique de l'identité sous un angle différent, afin que l'utilisateur accède simplement et efficacement à tous ces services. L'augmentation de la complexité crée un point de rupture qui oblige les organisations à envisager des solutions plus globales.

C'est dans ce contexte que le GTN-Q(Groupe de travail québécois sur les normes et standards TI pour l'apprentissage, l'éducation et la formation) s'est donné le mandat de :

- Préparer un recueil d'information destiné aux organismes de l'éducation afin de les renseigner sur les enjeux et moyens à mettre en œuvre pour assurer l'émergence d'une fédération d'identité.

- Consulter des représentants d'organismes des trois ordres d'enseignement qui explorent ou ont mis en œuvre ce type de mécanismes.

Pour y arriver, ce document aborde la problématique en ciblant dans un premier temps, à la section 2, les enjeux liés à l'utilisateur et aux systèmes éducatifs. Cette section s'adresse aux spécialistes des technologies, mais plus spécifiquement, aux gestionnaires et aux acteurs touchés de près ou de loin et qui voudraient comprendre ou influencer un processus consultatif ou décisionnel dans le cadre de la mise en place d'une fédération d'identité. Dans un second temps, le rapport cible les aspects techniques liés à des solutions technologiques applicables dans une fédération d'identité. Cette section s'adresse avant tout aux spécialistes des technologies qui ont des notions dans le domaine de la gestion d'identité. Dans la section 4 nous effleurons la démarche à entreprendre.

Il est important de noter que ce document se veut un déclencheur pour stimuler la mise en action des parties prenantes, menant à la réalisation d'une fédération d'identité. Ce recueil d'informations n'est pas une étude exhaustive du sujet.

Pourquoi une fédération

Mise en contexte

Les progrès technologiques des dernières décennies permettent l'échange d'informations à un rythme de croissance effréné. Le milieu de l'éducation doit s'adapter et intégrer les nouvelles technologies informatiques et de télécommunications. L'omniprésence des technologies dans nos vies personnelles et professionnelles crée des opportunités dans des proportions sans précédent.

Les écoles, centres, cégeps et universités sont maintenant à un carrefour où diverses parties prenantes doivent trouver une place, voire un équilibre, entre les services et la sécurité de leur identité. Toutes les parties prenantes subissent à divers degré des impacts dû aux bouleversements causés par la propagation rapide des diverses technologies. Il n'y a pas si longtemps, le périmètre d'action d'un établissement à vocation éducative se limitait à la communauté de proximité. L'avènement du web a tout changé. Nos processus de communication émergents sont à la fois multidirectionnels et ciblés. Ainsi nous souhaitons, comme utilisateur des plateformes, joindre des publics cibles non organisés et des regroupements qui sont, eux, déjà organisés, afin d'établir des canaux de communication qui rendront accessible l'information de façon efficiente et efficace. La problématique du contrôle des coûts et la sécurité des données s'imposent comme une priorité dans un contexte où l'accessibilité et la diversité des données augmentent de jour en jour.

La sécurité n'est pas le seul enjeu lié à la gestion de l'identité. La rareté des ressources ayant l'expertise nécessaire, les barrières culturelles, administratives et structurelles et les lacunes au niveau de la gouvernance sont autant de facteurs souvent sous-estimés dans des projets de fédération.

Avec le Web 2.0 et 3.0, la personnalisation de l'information dans les pages Web amène des questionnements qui doivent trouver, à moyen terme, des réponses efficaces. Comment assurer cette personnalisation de l'information, tout en préservant le respect de la vie privée de l'utilisateur? Face à ce contexte, un certain nombre d'enjeux se dessinent :

- Les usagers eux-mêmes et les organismes scolaires auxquels ils sont inscrits gèrent souvent plusieurs abonnements ou comptes avec des fournisseurs de services.
- Ces mêmes usagers et organismes scolaires doivent, malgré eux, divulguer des informations concernant leur identité.
- Les usagers ont une tendance marquée à utiliser les mêmes justifications d'identités pour les différents services ayant ainsi un impact sur la sécurité de leur identité respective.
- Il n'existe pas de véritable norme de gestion de l'identité par ou pour les organismes scolaires, hormis certains systèmes (GRICS, Skytech, COBA, etc.) qui standardisent un certain nombre de règles.

- Dans l'état actuel de l'implantation des technologies, on ne peut que très peu tirer parti du croisement des données pour donner à l'utilisateur des informations personnalisées.

- Les approches tirant parti des entrepôts de données et des systèmes de veille stratégique (*Business Intelligence*) ont besoin de données cohérentes, notamment celles liées à la gestion de l'identité et à ses attributs.

Une définition

Une fédération est une organisation virtuelle constituée d'un groupe d'organisations qui sont liées entre elles par des intérêts communs dans un ou plusieurs domaines d'affaires. Chaque organisation de la fédération est autonome et délègue à celle-ci la gestion des accès. Cette gestion permet l'authentification et l'autorisation des usagers selon un niveau de confiance défini par des politiques de la fédération. Une fédération repose à la fois sur une infrastructure informatisée et une architecture de services. Les services de la fédération offrent les opérations suivantes :

- Émission, validation et transmissions des informations relatives aux jetons, des demandes de justification, des attributs et des assertions relatives à la sécurité;
- Intégration des informations relatives à la sécurité;
- Application des politiques qui utilisent les informations relatives à la sécurité, afin de valider l'autorisation pour une demande ou une action sur une ressource ou un service.

Survol des acteurs impliqués

Une fédération d'identité permet de regrouper des organisations diverses afin d'offrir des services où l'accès sera géré selon des normes communes. Ces organisations sont composées, dans un premier temps, d'un certain nombre d'acteurs clés et autorités. Dans le cadre du mandat, nous nous limiterons à un survol de très haut niveau au niveau des acteurs.

L'autorité significative pour un utilisateur est l'organisation responsable d'émettre et de gérer au quotidien l'identité numérique des utilisateurs, qu'ils soient étudiants ou employés. Il s'agit, dans la majorité des cas, des commissions scolaires, cégeps et universités. Afin de ne pas alourdir le texte, les écoles privées, les écoles de formation spécialisées, les centres de formation générale des adultes, les centres de formation professionnels, les organisations dédiées à la formation à distance ne sont que quelques exemples d'entités regroupées sous le vocable d'organismes scolaires. Nous les citerons explicitement si nécessaire dans le reste du texte. Ces organismes offrent une panoplie de services numériques à leur clientèle.

Le deuxième acteur clé est, dans le cas qui nous préoccupe, le gouvernement du Québec et, incidemment, le MELS. Le MELS émet le code permanent. Il décide d'un certain nombre de règles et normes qui encadrent les organismes. Le gouvernement du Québec est un important prestataire de services. Son alignement stratégique et opérationnel est vital pour arriver à édifier des systèmes cohérents.

Les troisièmes acteurs importants sont les concepteurs des systèmes de gestion des ressources humaines et des systèmes de gestion de la vie étudiante. Mentionnons à titre d'exemple la Société GRICS pour les commissions scolaires, Skytech et COBA pour les cégeps. Ces systèmes offrent les sources de données permettant d'automatiser les processus de gestion des utilisateurs ainsi que leurs attributs.

Le quatrième acteur est l'utilisateur des services. Il s'agit des élèves, étudiants, enseignants, professeurs, professionnels, personnels de soutien, cadres, etc. C'est pour eux que sont mis en place d'abord et avant tout les services. Il est un acteur auquel on attribue plus ou moins d'autonomie pour décider des services utilisables.

Le cinquième acteur contient les parents des élèves du secteur jeune. Cette catégorie d'utilisateur, que l'on peut qualifier de membre externe, doit accéder à des services internes des organismes.

Le sixième acteur est constitué des services privés hébergés ou en ligne qui offrent des services gratuits ou payants. Dans cette liste très longue de services, il convient de différencier deux familles de services et d'applications : les applications coquilles et les applications incluant du contenu. Les applications coquilles sont, par exemple, les portails organisationnels. Les organismes achètent des coquilles telles que Édu-groupe, le Bureau virtuel et Omnivox et gèrent, dans ces coquilles, des contenus. Les applications incluant du contenu sont complètes en soi. Il existe également des applications mixtes qui peuvent augmenter la complexité de gestion de l'identité.

Comme septième acteur, il faut prévoir un ou des acteurs potentiels qui prendront en charge la fédération d'identité elle-même ou une sous-fédération. Par exemple, il serait envisageable de regrouper les fédérations éducatives de chacune des provinces dans une fédération canadienne. Chaque fédération éducative provinciale pourrait être constituée d'une fédération de l'enseignement supérieur et d'une fédération pour les commissions scolaires. Cette fédération pourrait exercer ses fonctions parallèlement à une fédération des services gouvernementaux, etc. Nous ne prétendons pas que ce soit un modèle souhaitable, mais la technologie permet d'envisager une telle approche.

Les institutions concernées

Plusieurs organismes à vocation éducative doivent pratiquer une gestion de l'identité au Québec. Voici un aperçu qui comprend l'essentiel des institutions concernées et nous sommes conscients de ne pas toutes les énumérer :

- 12 universités;
- 40 cégeps, sans compter les organismes secondaires rattachés;
- 69 commissions scolaires, plus 3 commissions scolaires à statut particulier;
- Près de 200 écoles privées membres de la Fédération des établissements d'enseignement privés.

Nous en arrivons donc à un total de plus de 300 institutions qui gèrent une identité numérique dans la province de Québec, selon des paramètres relativement distincts. Il eût été souhaitable, dans le cadre de cette étude, de dresser un portrait des pratiques de gestion mises en œuvre afin de connaître les références de départ au niveau des services d'annuaires et des pratiques mises en œuvre pour gérer l'identité. Cette tâche incombera à d'autres intervenants vu la portée du mandat actuel.

Prospectives d’avenir

Plusieurs visions pourraient être mises de l’avant pour justifier la nécessité d’une meilleure gestion de l’identité qui passerait par une fédération. Explorons ici quelques prospectives d’avenir qui mettent en valeur les avantages pratiques d’une fédération d’identité. Ces pistes sont des indicateurs d’orientations. D’autres avenues pourraient être envisagées.

La cohérence

Dans la dernière décennie, un nouveau terme, l'*architecture orientée services* (SOA), est apparu avec plusieurs concepts sous-adjacents. Cette architecture est un modèle de médiation et d'interaction. À l'origine, elle vise les problématiques d'interopérabilité entre les technologies informatiques distribuées au sein de nos entreprises. Un service est une réponse à un besoin et il est exécuté par une entité qui peut être, à l'interne, un département ou à l'externe, un fournisseur. Le client reçoit la réponse par le biais d'un médiateur.

Dans le domaine de l'éducation, une organisation scolaire dessert ses employés, ses enseignants ou professeurs, ses étudiants ou élèves avec plusieurs services : secrétariat, comptabilité, soutien technique, ressources humaines, transport, sécurité, services de l’enseignement, compagnie d'édition, etc. Chacun de ces services utilise des logiciels comportant des bases de données où chaque utilisateur a une identité et des attributs. Le cas qui suit souligne la différence entre une identité par service et une identité fédérée au sein d'une commission scolaire. Un utilisateur peut avoir plusieurs identités dans l’organisation. Voyons un cas limite parmi d’autres qui exprime cette réalité. Un étudiant inscrit à un centre de formation professionnelle est le parent de deux enfants qui fréquentent deux écoles dans deux commissions scolaires différentes. Il occupe aussi un poste d'employé de soutien au sein de l'une des deux commissions scolaires. Cet utilisateur (Étudiant-Employé-Parent) fait appel à autant de services qu'il peut posséder d'identités et de rôles dans un système ne comportant pas de principes de gestion d'identité fédérée. Tant pour lui que pour les commissions scolaires concernées, la gestion de son identité et la communication avec les divers services augmentent en complexité. La solution simple est de donner quatre identités à cet individu : étudiant à l’éducation des adultes, employé, parent à la commission scolaire A et parent à la commission scolaire B. Si la commission scolaire A a fait des travaux d’intégration plus poussés, il se pourrait qu’il accède aux informations via un seul compte, mais ce n’est pas assuré.

Maintenant, prenons pour hypothèse la présence d’une fédération au sein d'une architecture de services. L'individu possèderait alors un identifiant unique qui ne permet pas de déterminer aucun de ses attributs : âge, sexe, race, religion, rôle, emploi, etc. Il en va de même pour ses enfants. Son identité et celle de ses enfants mineurs sont transmises seulement lorsque la loi l'exige ou avec son consentement. Les attributs transmis sont régis de la même manière.

De l’identité aux entrepôts de données

Un organisme a pour mandat de soutenir, après les heures de classe, les élèves qui ont des travaux à faire et qui éprouvent des difficultés. Dans ce contexte, on souhaite connaître la proportion des élèves québécois du secondaire par région administrative qui recourent à ce service et qui sont à risque d’échouer un cours ou certaines notions plus problématiques.

Pour y arriver, il faut faire le croisement de plusieurs types de données. Ce croisement de données pour l’organisme en question pose un défi : les organismes scolaires ou le gouvernement veulent lui donner des statistiques globales, mais on ne veut pas lui transmettre l’identité de chacun des élèves impliqués dans le processus statistique. Il faut donc faire des croisements de données à partir de l’identité numérique de l’élève, l’utilisation du service, ses résultats scolaires, les matières pour lesquelles il a recouru à de l’aide, sa région administrative d’appartenance, etc. Dans le cas de l’identité des élèves, un mécanisme a été prévu et permet de préserver leur anonymat. Avec cette mise en œuvre et l’apport d’autres services technologiques, l’organisme est capable d’établir une évaluation exacte des services qu’il dispense aux élèves en difficulté.

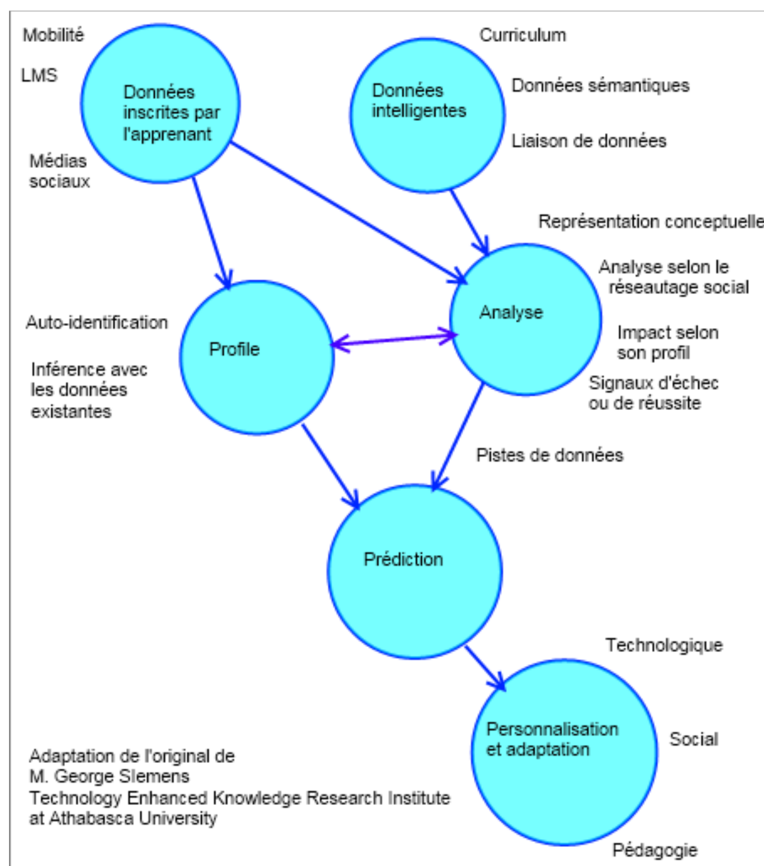
Encore plus loin

En ce qui concerne le livre numérique en classe sur des ordinateurs portables, l'imagination est probablement notre seule limite. Il existe déjà plusieurs applications dans le domaine commercial qui attendent qu'on leur ouvre la porte à nos classes!

Pourrait-on penser mettre à contribution une interopérabilité entre ces différents systèmes et une fédération d'identité pour évaluer le matériel pédagogique numérique et, plus particulièrement, les manuels scolaires numériques?

La réponse n'est pas simple, mais, oui, c'est envisageable. Le croisement des données de planification, de réussite éducative, des ressources utilisées pourrait permettre de dégager des tendances et des indicateurs de réussite en fonction de la fréquentation d'une ressource ou d'une combinaison de ressources, selon un profil d'apprenant, etc.

Bien que notre étude ne porte pas sur ce sujet, il est tout même important de remarquer que des chercheurs ont schématisé de tels processus d'analyse qui font appel à des données identitaires normées et au profilage. Voici un exemple de M. George Siemens, *Technology Enhanced Knowledge Research Institute*, Université d'Athabasca, qui va même plus loin et nous amène à la personnalisation et l'adaptation des apprentissages en fonction des analyses prédictives.



Ce schéma nous indique que l'interaction de nombreux systèmes devra s'opérer, dans certains cas en temps réel, afin de livrer des données immédiates. Sans une gestion de l'identité efficiente, chacun des systèmes impliqués devra prévoir des investissements considérables qui dépasseront à terme les investissements planifiés dans une fédération d'identité.

La recherche

Une fédération d'identité pourrait jouer un rôle clé pour permettre l'émergence de projets de recherche ciblée à coûts moindres. La cohérence des données identitaires permettrait de rendre accessibles des données qui demanderaient des moyens financiers hors de proportion.



Quelques exemples ici et ailleurs

Au Québec, nous n'avons retrouvé que deux familles de fédérations : clicSéQUR et l'implantation de Shibboleth dans deux universités : l'UQAM et l'Université McGill. ClicSéQUR est un service d'authentification gouvernementale du gouvernement du Québec. Selon nos constatations, il est fort probable que leur approche ne puisse pas répondre aux besoins spécifiques du milieu scolaire. La seconde famille regroupe, comme nous le disions, deux universités québécoises, mais également autour de 17 universités canadiennes. Bien que ces universités aient adopté des technologies qui permettent de mettre en place des services fédérés, il n'existe pas à proprement parler de fédération en dehors des murs de ces universités. Ils utilisent Shibboleth et, à ce titre, il leur serait possible de plus facilement se fédérer. Nous ignorons si toutes ces universités adhèrent présentement à une convention commune d'attributs. Mentionnons que CANARIE veut mettre sur pied un projet de fédération d'identité. D'autre part, dans le scénario éventuel de connexion entre les deux fédérations, un utilisateur authentifié par clicSéQUR aurait un jeton ayant le niveau d'assurance requis pour accéder à une fédération universitaire, mais pas dans le sens inverse. Le niveau d'assurance de la fédération universitaire est probablement de niveau deux alors que celui de clicSéQUR est de niveau trois. Un mécanisme supplémentaire doit établir le niveau d'assurance requis par un fournisseur ayant un niveau supérieur que celui établi lors de l'authentification initiale.

Il existe de par le monde plusieurs fédérations nationales. Les raisons et les motivations de leurs créations, leur gouvernance et leur mode de fonctionnement respectif varient grandement. Les fédérations de l'Espagne, du Danemark et, surtout, du Royaume-Uni ont particulièrement attiré notre attention due à la quantité et à la qualité de la documentation à leur sujet.

La fédération, selon la définition d'un espace numérique de travail du ministère de l'Éducation nationale en France, fait partie des services socles de l'architecture du système d'information et de communication. L'accès d'un usager à ce système est à la fois simple, dédié et sécurisé aux outils et contenus pour son rôle et son profil. Ainsi, la littérature concernant les fédérations traitées dans le rapport *Les plates-formes virtuelles d'apprentissage en Europe : que nous apprennent les expériences du Danemark, du Royaume-Uni et de l'Espagne? Panorama comparatif* n'adresse pas directement la gestion de l'identité et de l'autorisation, mais les technologies de l'information et de la communication dans un sens plus large. Il est quand même possible d'apprécier la mise en œuvre de la gestion de l'identité et de l'autorisation par déduction selon diverses perspectives.

Entre 2005 et 2009, l'Espagne a investi dans un programme d'Internet en classe. Les objectifs de ce programme étaient :

- Développer une infrastructure technologique (ordinateurs multimédias, périphériques et accès Internet dans les classes) et promouvoir des stratégies en faveur de l'insertion numérique;
- Financer l'achat d'ordinateurs pour les familles dont les enfants sont en âge scolaire;
- Donner des conseils techniques et pédagogiques et offrir un support aux écoles et aux associations d'enseignants;

- Encourager le développement, la diffusion et l'utilisation de contenus pédagogiques;
- Former les enseignants et les formateurs des enseignants;
- Assurer le suivi et l'évaluation des initiatives dans les écoles.

Le programme espagnol avait un budget de 454 millions d'euros pour cette période. Les outils et les approches ont été faits avec des logiciels libres. C'est dans ce contexte que s'est réalisé le projet de fédération d'identité.

Le Royaume-Uni a investi plus de cinq milliards de livres sterling entre 1997 et 2007 dont une partie a été affectée aux fédérations d'identités et à la gestion de l'identité. Durant cette période, le gouvernement britannique a transformé l'enseignement avec l'utilisation massive des technologies de l'information et de la communication. En 2002, une évaluation sur l'impact pédagogique, l'efficacité opérationnelle et l'incidence sur tout le secteur des TIC a mis en évidence l'insuffisance des infrastructures de communication, des problèmes à divers niveaux dans les nombreux sites Web et la compréhension problématique du rôle de l'industrie privée face aux ressources liées à l'apprentissage en ligne. Des objectifs similaires à ceux-ci ont été fixés par l'Espagne pour leur fédération. Il faut souligner que le site de la fédération du Royaume-Uni, http://www.ukfederation.org.uk/, est riche d'informations pertinentes et est cité très fréquemment. Nous sommes d'avis que les démarches et les processus de cette fédération sont des incontournables comme point de départ pour quiconque considère la mise en œuvre d'une fédération d'identité. Par exemple, dans la province de la Colombie-Britannique, la création d'une fédération pour tous les services gouvernementaux a présentement lieu et cette action nous laisse croire qu'ils se sont inspirés fortement du modèle du Royaume-Uni. Le site suivant http://www.cio.gov.bc.ca/cio/idim/index.page fait état des travaux. En effet, la littérature scientifique due au financement de plusieurs projets de la part du Royaume-Uni fait mainte fois référence à ses initiatives et ses approches.

Le Danemark a entrepris plusieurs projets nationaux. En 1998, un plan d'action sur cinq ans visait le développement de la connectivité, des ressources digitales et une évolution du rôle de l'enseignant. En 2001, une initiative stratégique a été entreprise pour la formation des enseignants, le partage des connaissances entre les établissements, l'utilisation des technologies de l'information et de la communication hors de l'école pour les enfants ayant des besoins spécifiques. Entre 2004 et 2008, l'accent a été mis sur le développement de l'équipement, des contenus numériques, d'un portail national, de tableaux blancs interactifs et la formation des enseignants. Les établissements ont toujours bénéficié d'une marge de manœuvre afin de tenir compte de leur environnement respectif.

Le mode de gouvernance du Danemark dénote la participation et la coopération de toutes les parties prenantes. Le partage des responsabilités est clair : le Ministère donne son appui, les autorités locales gèrent les projets de proximités et les établissements, avec leurs enseignants, sont directement impliqués pendant les projets de développements. En ce qui concerne l'Espagne, la gouvernance est très coopérative due à la constitution du pays qui donne une autonomie aux diverses autorités locales.

Les aspects techniques

Concepts clés et lexique

Une fédération s’appuie sur quelques concepts : l’identité fédérée, le partage des responsabilités, la relation de collaboration et de confiance entre les acteurs et la gestion des identités.

L’identité fédérée permet à deux ou plusieurs systèmes d’authentification différents de représenter un individu selon leurs éléments sécurisés respectifs, de telle manière que l’un ou l’autre des systèmes puisse accepter l’authentification effectuée par un autre.

Le partage des responsabilités au niveau d’une fédération est tri partite. Le fournisseur d’identité, en accord avec les politiques de la fédération, se charge de l’authentification et des processus associés : enregistrement, gestion des comptes, etc. Le fournisseur de services, avec les informations qui lui sont transmises par le fournisseur d’identités, accomplira le service demandé. Enfin, l’utilisateur bénéficie de ces deux fournisseurs.

La collaboration et la confiance entre les divers acteurs sont des valeurs essentielles pour l’existence d’une fédération. La qualité de service du fournisseur de services envers l’usager et celle entre le fournisseur d’identité et le fournisseur de services se doivent d’être garanties. Les nombreux aspects légaux doivent être adressés comme les moyens techniques pour la sécurité, la gestion des jetons de sécurité et les processus de validation de l’authenticité des informations mises en cause.

La gestion d’identités fédérées permet de simplifier la gestion des identités inter organisations, de faciliter l’intégration de nouveaux partenaires au sein de la fédération et de partager de l’information sécurisée, en plus d’offrir aux entreprises, aux gouvernements et aux individus un moyen plus sûr et plus pratique de contrôler les informations identitaires. Toutes les organisations, qu’elles soient ou non commerciales, peuvent y adhérer. De nos jours, elle est un élément essentiel au commerce électronique, au e-learning, aux services Web et aux services de données.

Outre les concepts, il est nécessaire d’avoir une connaissance du vocabulaire dans le domaine. Le reste de cette section fournit un bref lexique.

Un protocole d’authentification est un processus décrivant la transmission d’informations numérisées via un jeton, dans le but de vérifier l’identité d’un abonné ou prestataire d’un service. Lors d’une session d’authentification, les données peuvent être cryptées dans certains protocoles d’authentification.

Une revendication (*claim*) consiste normalement en une assertion, à l’intérieur d’un jeton, fait par une entité au sujet de titres de compétences pour elle-même, ou une autre entité, qui doit être validée par un protocole d’authentification.

Une assertion est un énoncé émis par un auditeur en autorité qui contient des informations sur l'identité d'un abonné. Cet énoncé peut contenir d'autres attributs de sécurité. Les assertions sont parfois signées et obtenues via un protocole sécurisé. Par exemple, les témoins de connexion (*cookies*) peuvent être des assertions ou bien contenir des références à des assertions.

Une signature numérique est le résultat d'algorithmes asymétriques utilisant deux clefs : l'une privée et l'autre publique. La clé privée est utilisée pour crypter un document électronique et la clé publique, pour le décrypter. Les signatures numériques offrent ainsi une protection d'authentification et d'intégrité.

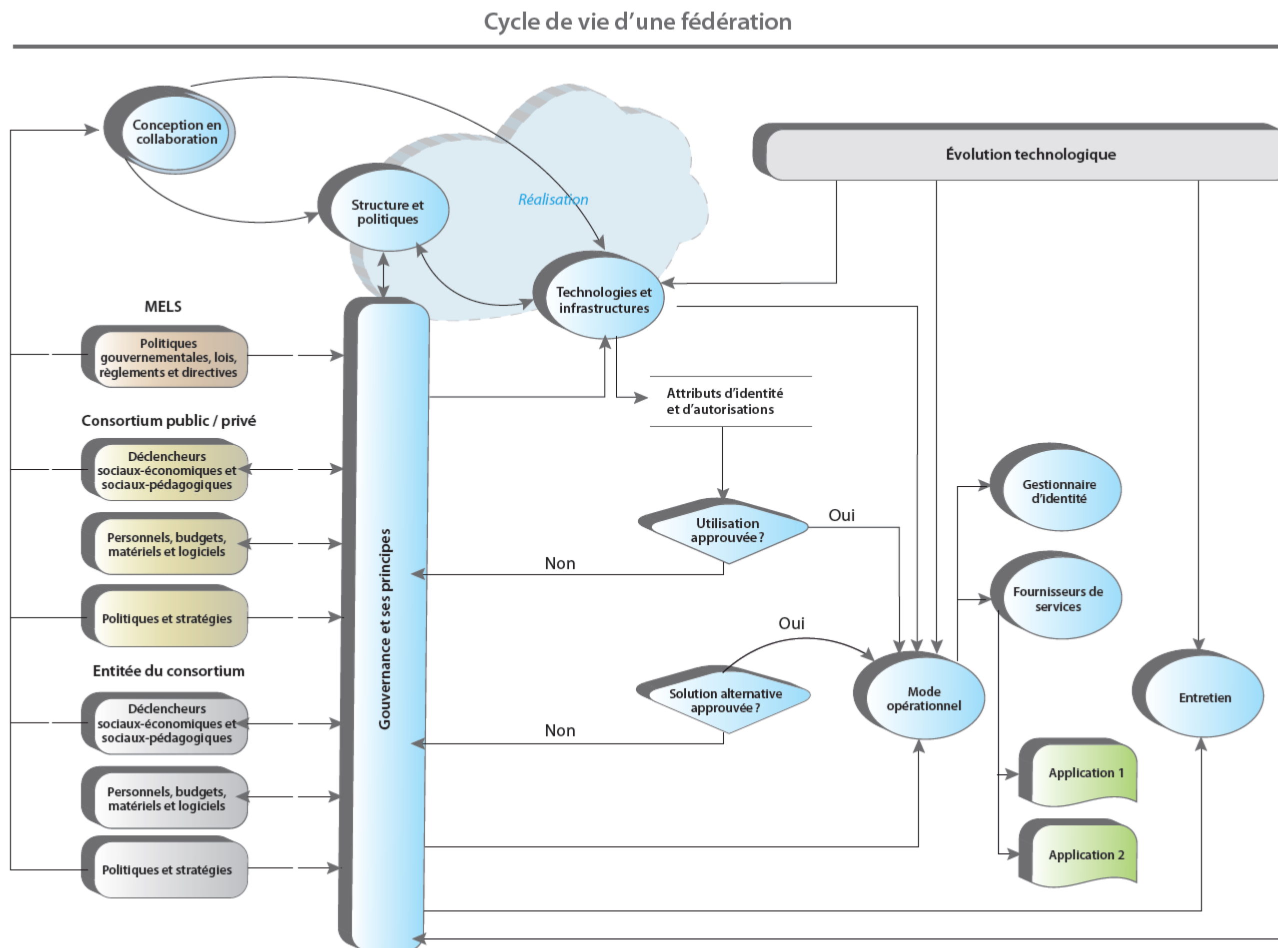
Shibboleth, par exemple, est à la fois un protocole d'authentification et un logiciel offrant des services connexes. Le protocole est fondé sur le langage SAML (Security Assertion Markup Language). Il est développé par un consortium d'universités américaines et est supporté par une communauté internationale.



Fonctionnement d’une fédération

Aspect opérationnel

Le fonctionnement d’une fédération est présenté selon deux perspectives dans ce document : technique et opérationnel.



Extrait et adapté du site http://beagle.rnet.missouri.edu/GPN/Docs/ [1]

La figure ci-dessus exprime la synthèse du cycle de vie d’une fédération qui pourrait s’appliquer dans le contexte québécois. C’est un processus continu et collaboratif à tous les niveaux. Dès que la planification et le contexte de la fédération sont établis, la conception collaborative débute. Les fondateurs de la fédération doivent, à cette étape, créer un cercle de confiance qui attirera de nouvelles organisations y ayant un intérêt. Le cercle de confiance est une organisation sociale

[1] GPN : Great Plains Network est un consortium d’universités du mi d’Ouest américain, qui permet à ses membres de se connecter au « National Research & Education infrastructure » et Internet2, et de faciliter l’utilisation des technologies de cyberinfrastructure pour tout le réseau.

dont les participants ont défini et accepté mutuellement les autorités, les responsabilités et les niveaux de confiance. Il est primordial de ne pas sous-estimer la complexité du problème : la compréhension de la gestion de l'identité selon les perspectives de la gouvernance, des politiques, de la législation, du déploiement des composantes et des divers services.

Il est très important de suivre les étapes et de déployer l'infrastructure seulement lorsque la solution de la gestion de l'identité est vérifiée, validée et que les objectifs poursuivis sont bien établis. Cette solution est la pierre angulaire de réalisation de la fédération. Dans le contexte de l'éducation au Québec, le ministère de l'Éducation du Loisir et du Sport est l'autorité principale de la gouvernance. Une autorité est une personne physique ou morale qui est membre de la fédération et qui est une source d'attributs de l'identité. Cela ne signifie pas nécessairement que le MELS doive faire la gestion quotidienne d'une fédération. Il s'agit plutôt de reconnaître qu'il est le seul à pouvoir orienter une stratégie qui s'appliquerait autant au secteur jeune qu'à l'enseignement supérieur.

L'autorité responsable d'une fédération d'identité est parfois reconnue par une législation, une politique gouvernementale, un contrat ou, tout simplement, par la nature de ses activités. Les divers services qui se situent dans l'infrastructure sont décrits plus loin, ainsi que leurs agencements, selon les principaux modèles qui existent. La gouvernance est sensible aux événements socio-économiques et socio pédagogiques dans la perspective de ses politiques. Ses ressources financières, matérielles et humaines proviennent des différents acteurs. Ces mêmes acteurs décident collectivement des politiques et des stratégies. Les parties prenantes se divisent en classe, la première étant le MELS. Ensuite, nous retrouvons le consortium public et privé constitué du gouvernement via ses ministères, les institutions du monde de l'éducation et des entreprises privées. Finalement, chaque entité est représentée dans la troisième classe afin de souligner son apport particulier. Le milieu scolaire, dans le contexte de la gouvernance, peut être un ou plusieurs de ses constituants : commissions scolaires, cégeps, universités, etc.

La gouvernance doit faire face à plusieurs défis ou enjeux tels que des restrictions légales issues des divers niveaux gouvernementaux, du respect de la vie privée, de la sécurité, de l'application des normes définissant les identités numériques selon les divers contextes en cause, de la définition des processus d'établissement des identités avec leurs juridictions respectives, de la gestion des processus et des services de la fédération. Afin de développer de manière cohésive un projet de fédération au sens large, le gouvernement de la Colombie-Britannique a adopté les lignes directrices suivantes :

- **Actions et artéfacts justifiables et proportionnés** : L'utilisation de l'identité numérique d'un individu par un organisme, un service ou un programme doit être faite en accord avec les lois en vigueur. En dehors d'une juridiction légale, son utilisation doit être faite avec le consentement de l'individu ou de son parent ou tuteur, le cas échéant. Le processus et les moyens employés pour l'authentification et l'autorisation d'un individu doivent être proportionnels au niveau de risque.

- **Respect du client, obtention de son consentement** : Il doit y avoir une raison spécifique pour obtenir d'un individu son consentement et de collecter des informations à son sujet. Celui-ci doit, autant que possible, gérer les attributs qui concernent son identité.

- **Informations limitées en quantité et par usage :** Une analyse des risques doit être faite tant sur les menaces internes et externes de la fédération. Lorsqu'une information est collectée pour un objectif spécifique, elle ne doit servir que pour celui-ci, à moins que la loi le permette.

- **Approche axée sur l'utilisateur et la consistance de son expérience** : Le client doit pouvoir naviguer dans les services ayant le même niveau d'assurance avec ses différents contextes (parent, employé et autre) avec le même SSO.

- **Support de la diversité des contextes de l'identité** : Le changement de contexte d'un fournisseur de service à un autre doit être possible à l'individu, selon ses choix.

- **Sécurité de l'environnement** : Les fournisseurs de service doivent aussi faire l'objet d'authentification afin que l'individu puisse avoir l'assurance que ses informations personnelles soient sécurisées. L'intégrité des données et leur exactitude doivent être une priorité pour la gouvernance de la fédération.

- **Transparence et impunité** : Les activités et les décisions en lien avec la gestion de l'identité doivent être communiquées en toute transparence et être compréhensibles pour toutes les parties prenantes. Les autorités de la fédération doivent être imputables et responsables de leurs actions. Les individus doivent être informés des risques qui découlent de l'utilisation d'une identité numérique.

- **Solution durable** : La solution retenue pour l'authentification et l'autorisation doit être modulaire et flexible. L'expression d'une norme ne doit pas impliquer une technologie plus qu'une autre. L'ajout de client ou de fournisseur ne doit pas affecter ces deux processus.

Par la suite, les attributs d'identité sont déterminés et transmis en accord avec les diverses politiques de la gouvernance. Les non-conformités aux diverses politiques ou aux normes adoptées par la gouvernance doivent être soumises à l'autorité ou aux autorités compétentes de la gouvernance. La technologie, par son apport, a un impact à tous les niveaux.

Aspects techniques

Il existe plusieurs modèles de fédérations qui peuvent être expliqués en termes d'agencements de divers services basés sur des concepts qui sont décrits dans cette section. La fédération, ou la gestion de l'identité fédérée émanent du besoin de permettre aux individus d'utiliser une identification unique pour accéder à des réseaux ou des services de plusieurs entreprises et organismes afin d'exécuter diverses transactions. En bénéficiant d'une telle portabilité, les individus ont une facilité accrue d'accès tout en contrôlant les informations concernant leur identité. Les entreprises, pour leur part, peuvent augmenter la portée de leurs réseaux et inclure les individus de la communauté fédérée dans leur périmètre de sécurité respectif. L'identité dans une fédération est gérée d'une manière unique au travers des domaines de sécurité des entreprises. Deux principaux concepts de sécurité doivent être préalablement définis : le domaine de confiance et la justification d'identité.

Un domaine de confiance (*trust realm*) est un espace sécurisé et administré dans lequel la destination d'une demande détermine et accorde des titres de compétences, selon les informations de sécurité fournies par la source et les politiques de la destination. Une justification d'identité (*credential*), ou un titre de compétence est une preuve de qualification, de compétence ou une habilitation de sécurité en provenance d'une entité d'un réseau (ressources, personne, rôle, service, etc.) duquel un attribut de sécurité peut être déterminé. Ainsi, la fédération peut être définie comme étant un ensemble de domaines de confiance qui ont un degré de confiance entre eux. Le degré de confiance, ou niveau d'assurance peut varier entre les domaines de confiance selon les besoins spécifiques et les ententes.

Deux processus principaux existent dans une fédération : l'authentification et l'autorisation. Le premier permet d'établir la confiance dans les informations qu'un usager présente pour s'identifier à un système informatique et, le second, les actions permises de l'usager. Les messages véhiculés entre les diverses entités de la fédération sont supportés par les services de celle-ci. Les interfaces et les protocoles sont fournis par la fédération dans le but d'émettre, de crypter, de valider et d'échanger des jetons. Ces derniers encapsulent des demandes de l'usager qui peuvent inclure, mais sans y être restreint, des attributs liés à l'identité et l'authentification.

Une fédération de base est exprimée par une agrégation de trois services : serveur de règles, service de jetons de sécurité et service de traitement des titres de compétences. La figure suivante extraite de Djordjevic illustre cette agrégation.

Le service de jeton (*security token service : STS*) de sécurité émet, valide et transmet les jetons de sécurité. Selon le format utilisé, le jeton peut comprendre plusieurs demandes, inclure des informations additionnelles et fournir la signature numérique. La validation d'un jeton diffère de celle des titres de compétences. Un jeton valide peut avoir des demandes dont les titres ne sont pas valides. Il y a aussi le transfert de jeton qui existe dans une fédération. Le transfert de jeton résulte de l'émission d'un nouveau jeton, suite à la validation d'un autre.

Le service de traitement des titres de compétences (*Credential processing service : CPS*) permet, en distinguant les attributs de sécurité internes ou externes par rapport au domaine de confiance, de gérer les certificats. Il traduit ou subsidiairement transfert des titres de compétences externes

en termes de compétences du domaine de confiance. La signification et l'interprétation des titres de compétences et des attributs de sécurité émanent d'un accord bilatéral entre un demandeur et un membre du domaine de confiance ou de la médiation d'un tiers. Ce type de service est nécessaire pour maintenir l'autonomie des domaines de confiance au sein d'une fédération. Ce service, avec une autorité d'enregistrement, participe au processus de validation/épreuvage de l'identité (*identity proofing*). Par ce processus, l'identité unique d'un individu est validée avec les informations nécessaires et suffisantes.

Le service d'application décisionnel des politiques (*Policy decision point : PDP*) gère la divulgation et la distribution des informations concernant les identités et leurs attributs de sécurité. Cette gestion s'exécute en accord avec les ententes entre les fournisseurs d'identités d'une part et des fournisseurs de services d'autre part.

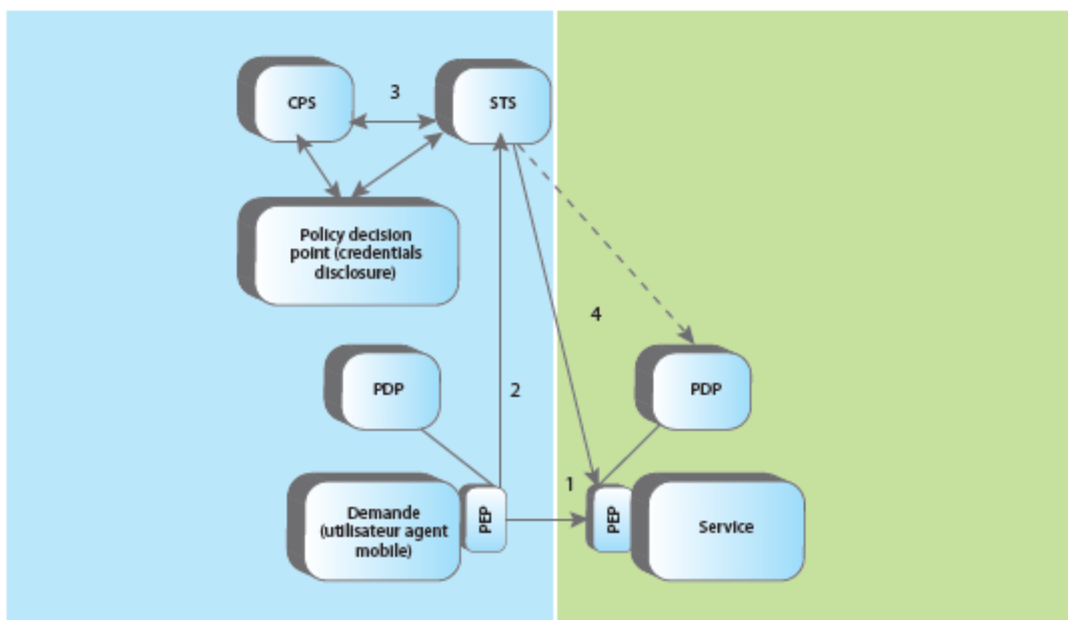
Le service d'application des politiques (*Policy enforcement point : PEP*) fait référence aux mécanismes qui appliquent les politiques de sécurité d'un domaine de confiance. Les messages entrants et sortants d'un domaine passent nécessairement par un ou plusieurs PEP. On retrouve souvent les PEP sur des nœuds de réseaux tels que des routeurs, des traducteurs de protocoles (pont) et des pare-feux. Un PEP peut utiliser un certain nombre de STS, CPS et PDP à l'intérieur d'un domaine de confiance, afin d'appliquer différentes actions selon les politiques.

Généralement, le choix d'un STS découle du type de jetons requis et le choix d'un CPS, des attributs de sécurité. Le type d'action autorisé influencera le choix du PDP. Les modèles de fédération diffèrent par les liens entre le PDP et les autres services STS/CPS/PDP.

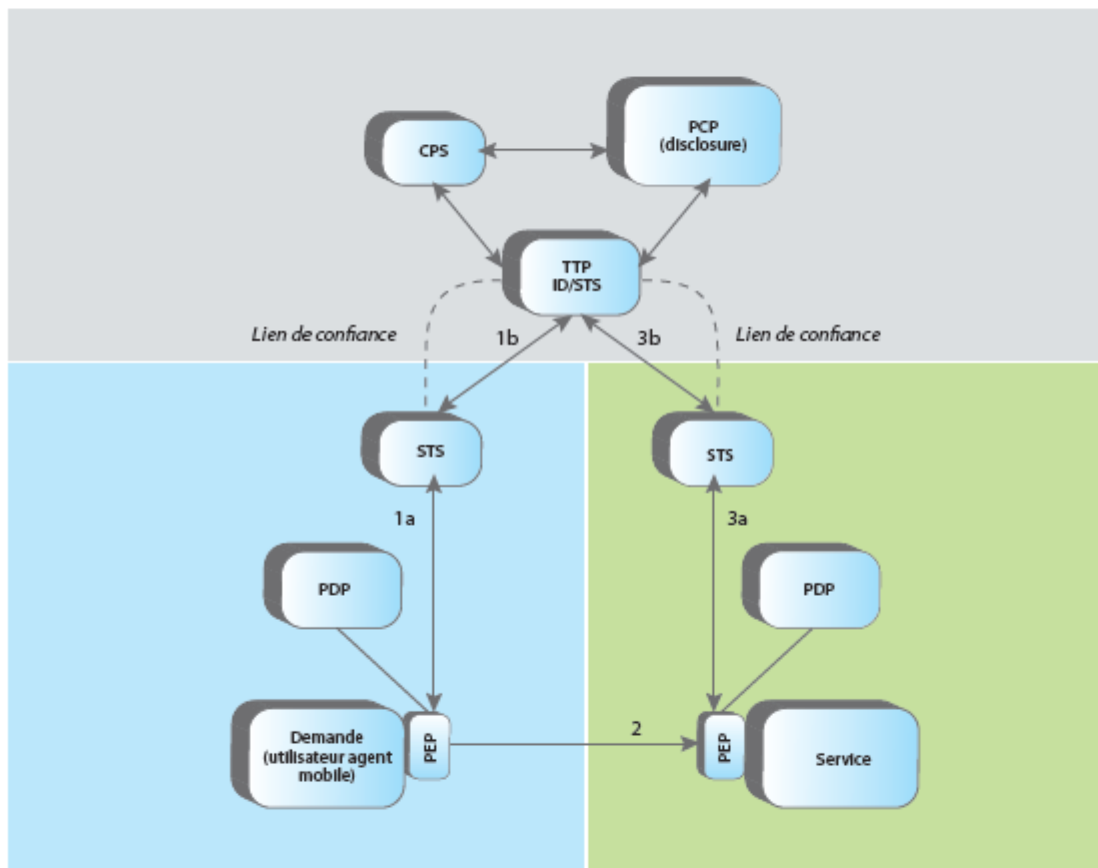
Modèles de fédération

Voici trois exemples de modèles de fédérations : Shibboleth, Liberty ID-FF et WS-Federation. Chaque image montre de deux à trois domaines de confiance. Les modèles Shibbolteh et WS-Federation en possèdent deux, alors que Liberty Alliance en possède trois. Le modèle Shibboleth présente une architecture qui est centralisée sur le domaine d'où vient l'utilisateur. Dans le cas où celui-ci désire accéder au service d'un fournisseur de la fédération, ce dernier entamera un processus WAYF (*Where are you from?*). Ce processus consiste à demander à l'utilisateur sa provenance et de demander à cette autorité deux choses : d'authentifier l'utilisateur et de fournir les attributs d'autorisation nécessaire au fournisseur de service en cause.

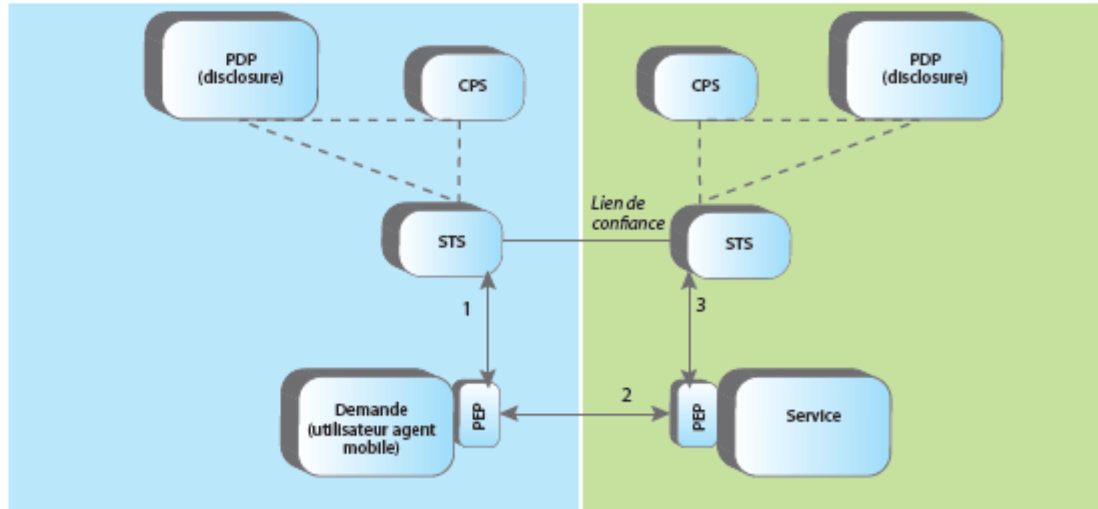
Le modèle selon Liberty sépare la responsabilité de l'authentification permettant ainsi de confier à un tiers ce processus. Liberty Alliance est plus commercial que Shibboleth. Toutefois, il semble que Microsoft et IBM ont jusqu'à maintenant refusé de se joindre comme membre. De plus, mentionnons qu'IBM s'implique au niveau de Shibboleth. Il y a évidemment plusieurs similarités avec Shibboleth dû à l'implication de la norme SAML. Toutefois, Liberty supporterait des fonctionnalités que Shibboleth ne supporte pas tel que le SSO pour les mobiles. Les divers agencements des services décrits plus tôt permettent de distinguer les diverses architectures. Le premier déclencheur dans chacun des cas est le service d'application des politiques (PEP). La nuance est dans le nombre et la disposition des autres services. Selon l'application de la fédération et les exigences de son déploiement, l'un ou l'autre des modèles sera préférable.



Architecture du modèle Liberty



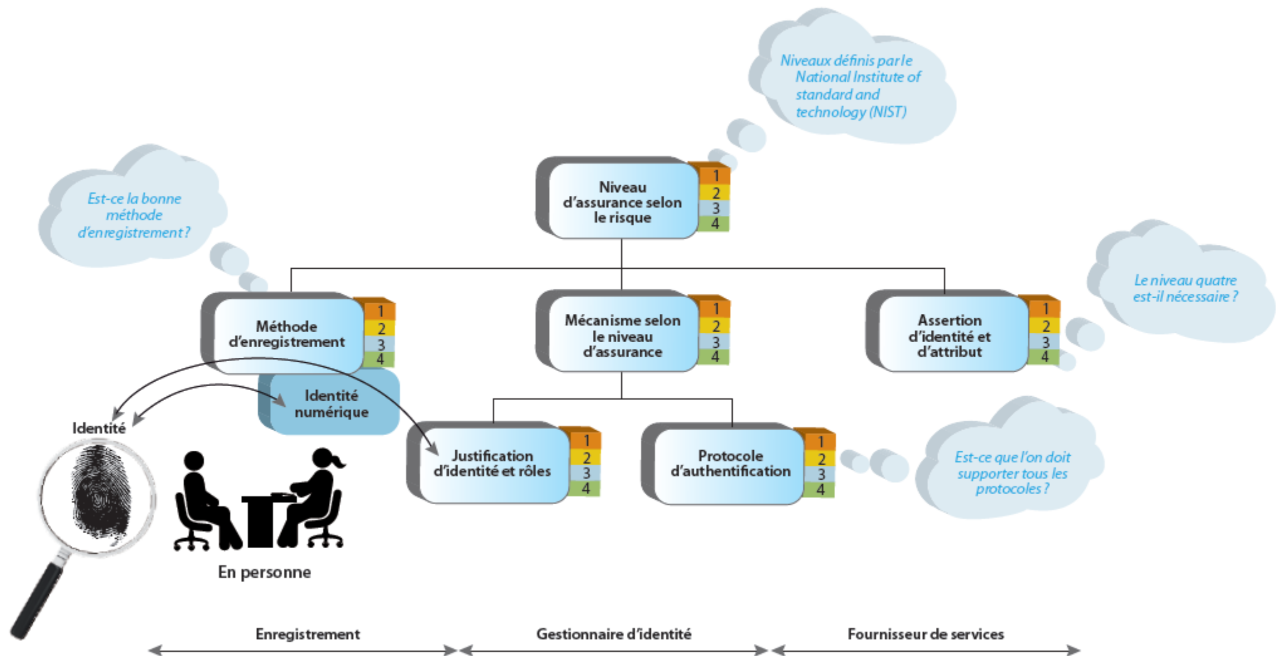
Architecture WS Federation / Modèle « STS » alternatif



L'architecture de WS-Federation a la possibilité, contrairement aux deux autres, d'avoir plusieurs configurations possibles. Une seule de ces configurations est présentée. Toutefois, nous devons noter que cette architecture n'est pas utilisée, à notre connaissance, dans une fédération dans le milieu scolaire. L'utilisation d'une architecture flexible telle que WS-Federation pose des défis importants au niveau des couts de gestion et de maintenance.

Cycle de vie d’un utilisateur dans le modèle Shibboleth

Naissance de l’identité numérique



Opérationnellement, nous présentons comme exemple l’approche de Shibboleth pour le cycle de vie d’un utilisateur. Le premier processus est l’enregistrement. Il est nécessaire qu’un organisme gouvernemental, ou un de ses délégués, rencontre en personne le citoyen afin que ce dernier prouve, à l’aide des documents requis, son identité. Les documents requis peuvent être l'extrait de naissance ou de citoyenneté ou tous autres documents reconnus. Lorsque l’organisation a établi avec certitude l’identité du citoyen, le justificatif d’identité lui est attribué. Son identité numérique existe dès lors.

Le second processus débute lorsque le citoyen utilise son identité numérique. L’organisation doit alors s’assurer que l’identité utilisée correspond au citoyen en cause. L’authentification, selon le niveau d’assurance demandé, utilise des mécanismes et des technologies pour valider l’identité.

Le troisième processus s’enclenche dès que le citoyen est positivement authentifié. Le citoyen, selon les attributs obtenus lors de son enregistrement, obtient le droit d’utiliser l’un ou l’autre des services disponibles dans la fédération.

Les objectifs de Liberty Alliance ou de Shibboleth relèvent d’une volonté de partager des usagers ou des clients. En effet, la gestion de l’identité simplifie l’accès, améliore l’ergonomie, facilite la navigation, etc. Pour les fournisseurs de services, l’avantage est d’abord la simplification de l’accès, surtout ceux qui n’ont pas à être identifiés par eux-mêmes. Toutefois, au niveau de la sécurité, Liberty Alliance n’est pas centralisé et devient par le fait même une cible mieux protégée contre les attaques.

Quelques normes et protocoles

Plusieurs normes et protocoles en matière de sécurité des systèmes d'informations existent. Elles sont de bons guides et, en ce sens, fournissent une assurance pour une démarche cohérente en ce qui concerne la sécurité. La norme ISO 27001, publiée en 2005, définit la Politique de gestion de la sécurité des systèmes d'informations au sein d'une entreprise. Cette norme comprend les domaines de processus suivants :

- définir une politique de la sécurité de l'information;
- définir le périmètre du système de gestion de la sécurité de l'information;
- réaliser une évaluation des risques;
- gérer les risques identifiés;
- mettre des mesures de contrôles en place.

Il y a aussi d'autres normes qui doivent potentiellement être prises en compte. En voici quelques-unes :

- ISO/IEC TR 14516 : 2002 Technologies de l'information -- Techniques de sécurité -- Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance
- ISO/IEC TR 18028-2 : 2006 Technologies de l'information -- Techniques de sécurité -- Sécurité de réseaux TI -- Partie 2 : Architecture de sécurité de réseau
- ISO/IEC TR 18028-3 : 2006 Technologies de l'information -- Techniques de sécurité -- Sécurité de réseaux TI -- Partie 3 : Communications de sécurité entre réseaux utilisant des portails de sécurité
- ISO/IEC FCD 24714-1 Technologies de l'information -- Adaptabilité et accessibilité individualisées en e-apprentissage, en éducation et en formation -- Partie 1 : Cadre et modèle de référence
- ISO/IEC FCD 24714-2 Technologies de l'information -- Adaptabilité et accessibilité individualisées en e-apprentissage, en éducation et en formation -- Partie 2 : Besoins personnels en matière d' « accès pour tous » et préférences de prestation numérique
- ISO/IEC FCD 24714-3 Technologies de l'information -- Adaptabilité et accessibilité individualisées en e-apprentissage, en éducation et en formation -- Partie 3 : Description des ressources numériques relatives à l'« accès pour tous »

Le langage SAML (*Security Assertion Markup Language*) est une norme développée par OASIS (*Organization for the Advancement of Structured Information Standards*). La version 2.0 a été approuvée en mars 2005. Cette version inclut l'apport de la version 1.0 de SAML, de la norme ID-FF (*Identity federation framework*) et du système Shibboleth avec son approche issue du milieu universitaire américain. Les métadonnées de SAML définissent un schéma XML et un ensemble de règles de bases pour le déploiement et la mise en œuvre de solutions pour les projets de

fédérations. Le format XML des messages de cette norme, appelé assertion, permet l'échange sécurisé des informations utilisées lors des processus d'authentification et d'autorisation. Trois types de déclarations sont fournis par SAML : authentification, états et décision d'autorisation.

Les deux tableaux suivants présentent le SAML selon ses relations avec d'autres protocoles et son historique.

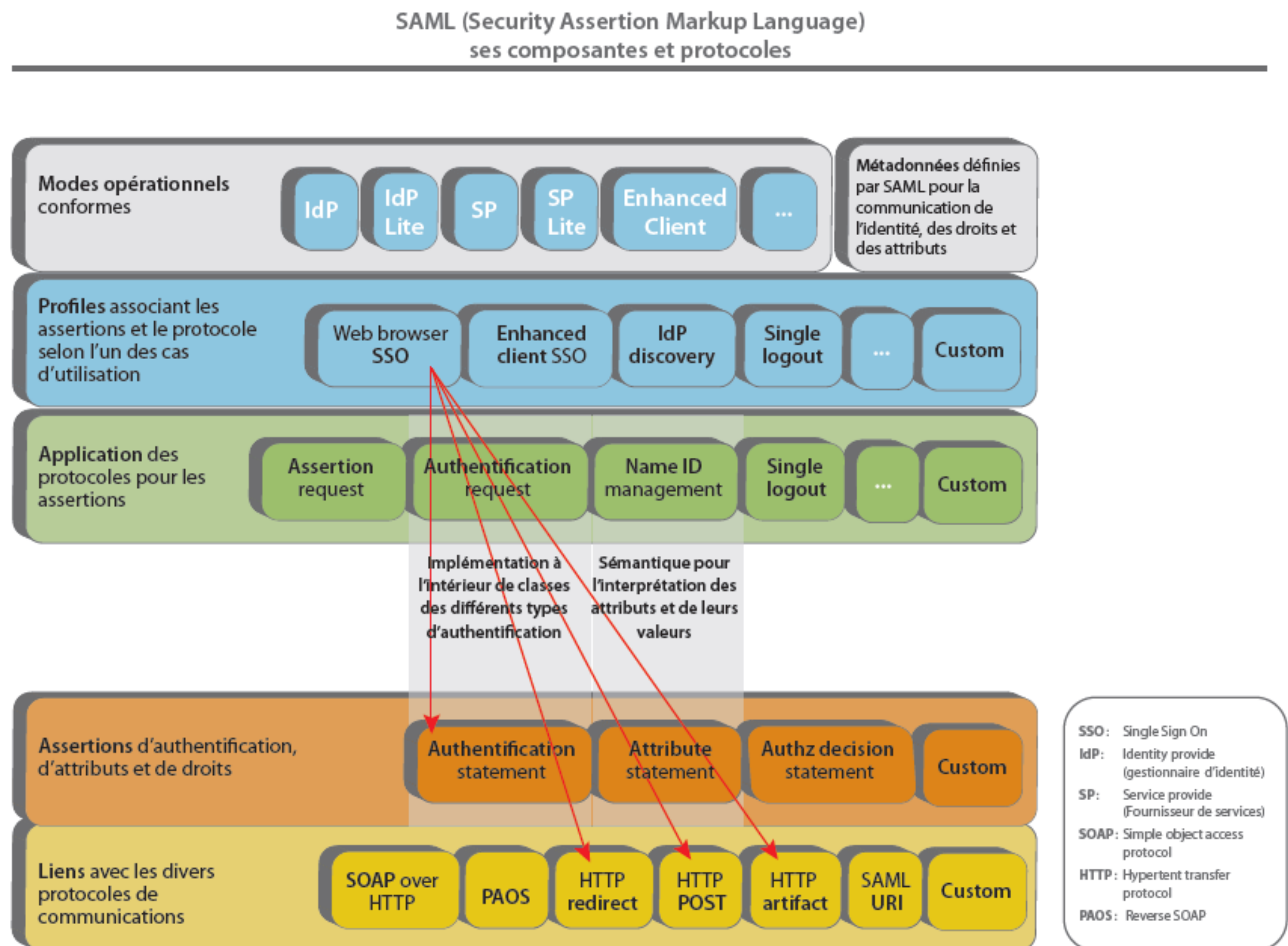


Image extraite et adaptée de http://www.xmlgrrl.com/blog/2007/02/26/saml-parfait/

Le SAML a une position dominante grâce à l'acceptation de l'industrie et les déploiements d'identité fédérée. SAML est déployé dans plusieurs milliers de *Cloud Single Sign-On* (SSO). Plusieurs grandes entreprises, agences gouvernementales et fournisseurs de services l'ont choisi comme leur protocole standard pour communiquer les identités à travers l'Internet.

Deux concepts essentiels sont définis : le fournisseur de service (*SP : Service Provider*) et le fournisseur d'identité (*IdP : Identity Provider*). Un troisième concept existe et sert d'outils de sélection lorsque plusieurs domaines de confiance existent au sein d'une fédération : service d'exploration (*DS : discovery service*). Le profil le plus couramment utilisé pour l'accès est l'authentification unique via un navigateur (*Web Browser SSO : single sign-on*). Ce profil consiste à

utiliser des redirections du navigateur Internet. Les différentes redirections possibles sont décrites dans la section *Architectures de bases des fédérations*.

Le protocole SOAP (*Simple Object Access Protocol*) est utilisé par SAML pour décrire la manière dont les applications communiquent entre elles. En fait, depuis la version 1.2, le SOAP est inclus dans le XML. Deux spécifications du XML sont utilisées respectivement pour le cryptage des données et la signature : *XML encrytion* et *SML Signature*.

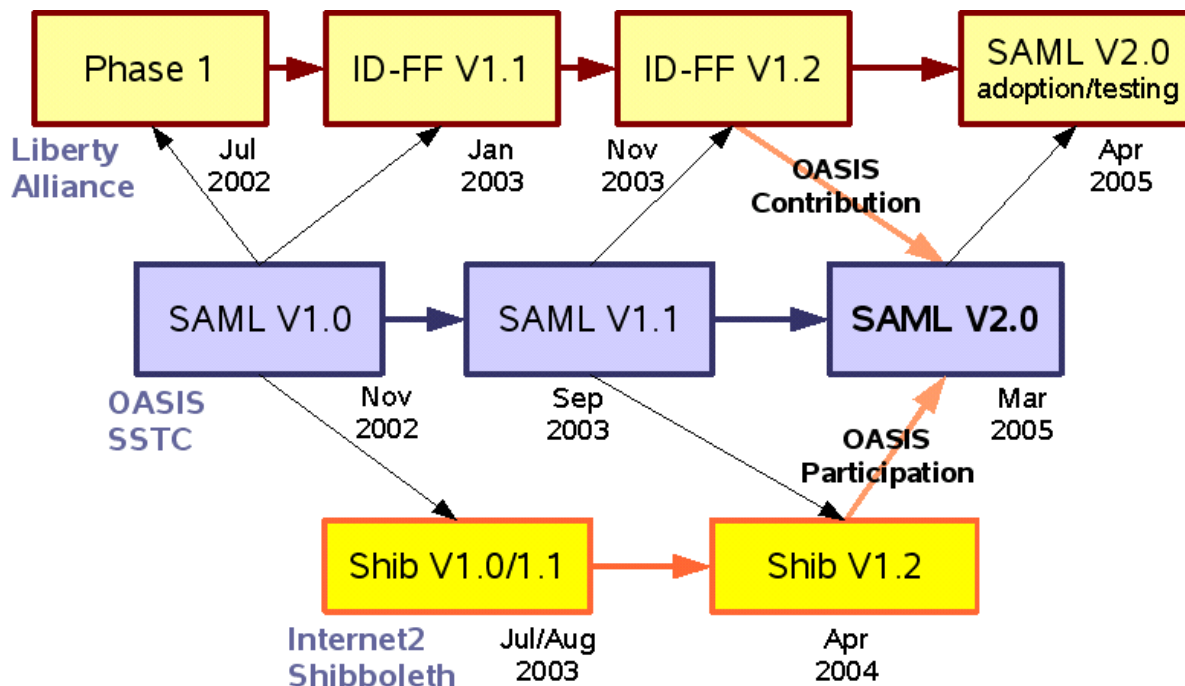
Les services de fournisseur d'identité et de services sont des exemples de modes opérationnels pour une utilisation dans les tests de conformité et de demande de proposition. Des métadonnées permettent de définir les données nécessaires que les fournisseurs demandent.

Voici une liste d'organisations qui travaillent actuellement sur des normes concernant la gestion de l'identité :

- OpenID foundation http://openid.net
- OAuth http://oauth.net/ (Cette norme est utilisée entre autres par Twitter, Google et Facebook.)
- Internet Engineering Task Force http://www.ietf.org/
- World Wide Web Consortium http://www.w3.org/
- Organisation for the Advancement of Structured Information standards http://www.oasis-open.org/
- US National Strategy for Trusted Identities in Cyberspace http://www.nist.gov/nstic/
- Open Identity Exchange http://openidentityexchange.org/
- Kantara Initiative (project of Liberty Alliance) http://kantarainitiative.org/
- InCommon Federation http://www.incommon.org/about.html
- US National Institute of Standards and Technology http://www.nist.gov/index.html
- Identity Commons http://www.idcommons.net/
- Information Card Foundation http://informationcard.net/foundation
- International Telecommunications Union http://www.itu.int/ITU-T/studygroups/com17/index.asp

International Organization for Standardization http://www.iso.org/iso/home.html

Bref historique de SAML 2.0



Liberty Alliance a été créé en 2001 par une trentaine d'organisations dans le but de rédiger des normes ouvertes, des lignes directrices et de meilleures pratiques de gestion des identités. Aujourd'hui, cette organisation continue avec les mêmes objectifs et un réseau mondial de plus de 150 organisations. Parmi ces dernières, on retrouve des sociétés confrontées aux consommateurs, les organisations éducatives, plusieurs gouvernements du monde entier, des centaines d'autres organisations dont la participation contribue à ouvrir plusieurs groupes communautaires intérêts spéciaux (GIS) autour de Liberty. L'OASIS Interoperability Lab est parrainé par le *General Services Administration* du gouvernement des États-Unis.

L'interopérabilité donne au SAML un énorme avantage sur les mécanismes de SSO propriétaires qui nécessitent que le fournisseur d'identité (IdP) et que le fournisseur de services (SP) utilise le même logiciel. Pour une entreprise, cela signifie que chaque nouvelle connexion nécessite la mise en œuvre de modifications des logiciels potentiellement nouveaux et différents. Avec le SAML, une seule implémentation SAML SSO peut supporter des connexions avec de nombreux partenaires au sein d'une fédération ou, même, de plusieurs. Certaines organisations, en particulier celles qui se doivent de soutenir de multiples implémentations propriétaires SSO, n'ont d'autres choix que l'utilisation de SAML pour Internet SSO avec *Software-as-a-Service* (SaaS).

La principale différence entre un système intra organisationnel et un système inter organisationnel est la protection des renseignements personnels. Le système Shibboleth, par sa conception, permet un contrôle de l'émission des renseignements personnels qui sont communiqués. Les fournisseurs de services ne reçoivent que les informations des utilisateurs nécessaires pour la prise de décision dans leur processus de contrôle d'accès. Par exemple, si une preuve d'adhésion est suffisante pour accéder à un service alors seulement cet attribut sera transmis. Plus

concrètement, un fournisseur pourrait vouloir connaître le cégep que fréquente un utilisateur, mais pas son identité et son mot de passe, pour vérifier si l'institution est abonnée à son service. Le logiciel Shibboleth IdP est un sous-système de gestion des politiques concernant l'émission d'attributs. La gestion de ces politiques est souvent un fardeau. Shibboleth fournit des outils pour établir les références et, ainsi, faciliter le contrôle de l'administrateur. La gestion des renseignements personnels est ainsi grandement facilitée.

Le système Shibboleth est un logiciel libre, utilisant des termes de licence non restrictive pour promouvoir son adoption à grande échelle dans les produits à code source ouvert et propriétaires. Avec un nombre croissant de partenaires et l'adoption croissante de la communauté internationale, le projet Shibboleth a reconnu la nécessité d'élargir la participation dans son processus de gouvernance, en particulier pour coordonner les nouveaux investissements importants dans le système.

Dans le cadre de ce rapport, nous avons choisi de privilégier l'examen de Shibboleth pour les raisons suivantes. Ce système a été développé dans le milieu universitaire. Il utilise la norme SAML et demeure une référence en ce sens. Le système Shibboleth supporte les applications Web et la gestion de l'identité et des accès au sein de plusieurs organisations. Ce système a une communauté très élargie lui procurant ainsi une pérennité certaine. Son design respecte plusieurs normes assurant ainsi un haut niveau de qualité. Ce même design ne vous permet pas de le lier à vos applications de manière intrinsèque. Autrement dit, vous pouvez intégrer Shibboleth dans vos applications Web sans avoir à leur apporter des changements importants. En ce qui concerne les autorisations, Shibboleth convient parfaitement aux applications du milieu de l'enseignement puisqu'il se base sur les attributs des utilisateurs pour le faire.

Les données liées à l'authentification

Un profil dans le contexte d'une fédération est défini dans la plupart des cas par le patron RBAC (*Role-Based Access Control*). Nous pouvons accéder aux détails du concept sur le site http://csrc.nist.gov/groups/SNS/rbac/.

Les données nécessaires à une fédération d'identité sont contenues dans des référentiels ou des bases de données. La mise à jour de ces données est effectuée lors de la gestion des utilisateurs, des politiques de sécurité et des mots de passe. Il est important de noter que les bases de données ou les référentiels des habilitations contiennent qu'une partie des données utiles à la fédération. Ainsi, les annuaires de sécurité contribuent au processus d'authentification et, parfois, d'autorisation, mais ne contiennent pas généralement les informations sur les profils. Les annuaires du type LDAP (*Lightweight Directory Acces Protocol*) renferment toutes sortes de données : nom, prénom, numéro de téléphone, adresse civique et de courriel, etc.) Il y a ensuite les divers NOS (*Network Operating Systems*) qui contiennent aussi ces données. On retrouve dans les systèmes d'exploitation réseau Windows server 2008, UNIX, Linux, Mac OS X et Novell Netware, entre autres. Bien sûr, il existe une multitude de systèmes informatiques qui permettent la gestion des identifications et des droits qui peuvent aussi servir de référence dans une fédération.

Une fédération implique une gestion centralisée des habilitations des utilisateurs. Les concepts de rôles applicatifs et de profils d'utilisateurs sont incontournables.

Une fédération implique que la gestion des identités traverse la sécurité des domaines qui la constituent. Contrairement à une gestion plus traditionnelle de l'identité, la gestion d'identité fédérée soulève de nombreuses questions complexes au niveau sociétal, entrepreneurial et technologique. Adhérer à une fédération nécessite que les organisations reconnaissent et identifient que des informations d'identité numériques existeront au-delà de leurs frontières, échappant ainsi à leur unique contrôle. En conséquence, les organisations auront à traiter des questions comme la responsabilité, la confidentialité et la confiance, l'investissement dans le développement de nouvelles technologies de l'application, l'élaboration d'un processus de collaboration au niveau des accords, la gestion de la divulgation d'informations critiques et la sécurité des transactions interentreprises.

Utilisation pour l'accès aux ressources

La gestion de l'identité, telle qu'appliquée dans une fédération, facilite l'informatique en nuage. Ainsi, le concept de nuage privé devient une alternative plus attrayante. Une entreprise ou un organisme qui possède un parc informatique ayant une capacité de calcul non utilisé à certaines périodes de temps, et faisant partie de la fédération, peut alors le mettre à la disposition d'autres membres.

Croisement des données

Grâce à l'accès unique qui facilite la collecte de donnée, l'aide à la décision est alimentée par des informations plus précises et ciblées. La propagation sécurisée de l'information est exécutée dans un contexte mieux contrôlé. Par exemple, des statistiques peuvent être compilées en respectant la vie privée des individus par une utilisation adéquate des attributs transmis via les assertions. Le croisement des données est certainement facilité, mais les possibilités de l'accès des données vont au-delà de la veille stratégique (*business intelligence*). L'informatique décisionnelle (en anglais : DSS pour Decision Support System ou encore BI pour Business Intelligence1) désigne les moyens, les outils et les méthodes qui permettent de collecter, consolider, modéliser et restituer les données, matérielles ou immatérielles, d'une entreprise en vue d'offrir une aide à la décision et de permettre aux responsables de la stratégie d'entreprise d'avoir une vue d'ensemble de l'activité traitée[2]. Dans le contexte de l'éducation, cette veille dépasse obligatoirement la seule perspective économique. Eurydice, le réseau d'information sur l'éducation en Europe, a publié plusieurs enquêtes dont l'une qui vise à évaluer les défis que les jeunes doivent relever pour se préparer face à une société de l'information. Les extraits suivants du document *Compétences clefs; Un concept dans l'enseignement général obligatoire* (octobre 2002) permet de considérer le croisement des données sous une perspective plus compatible avec l'enseignement :

« *Aujourd'hui, une importance considérable est par ailleurs accordée aux TIC et aux langues étrangères. Selon l'objectif qu'elles poursuivent, les compétences dans ces domaines sont classées comme académiques, techniques, génériques ou sociales. Les progrès de la technologie des télécommunications et des microprocesseurs ont élargi, intensifié et modifié la manière dont nous communiquons. Les TIC ont révolutionné les affaires, l'administration publique, l'éducation et le foyer. L'étendue de leurs implications économiques et sociales a fait de l'accès universel à l'informatique et à Internet une priorité absolue. En raison du volume d'informations disponibles en ligne, l'aptitude à accéder, à sélectionner et à gérer les données utiles est considérée comme une compétence clé. La culture informatique, ou utilisation concrète et rationnelle des TIC est la clé d'une participation réussie à la société de l'information. La maîtrise des TIC fait également office de catalyseur pour l'aptitude à la lecture, à l'écriture, au calcul.*

Et à de nombreuses compétences disciplinaires. La connaissance des pratiques de la messagerie, du courrier électronique et des salles de conversation est une compétence sociale pour tout

---

[2] Source Wikipédia http://fr.wikipedia.org/wiki/Informatique_d%C3%A9cisionnelle

utilisateur du cyberespace. Des carences dans l'accès en ligne et une compétence en TIC insuffisante chez certains groupes de population peuvent avoir des répercussions sérieuses pour la cohésion sociale en créant une fracture numérique entre les privilégiés et les exclus de l'information.»

Forcé de reconnaitre l'inégalité de l'accès à diverses ressources en télécommunication des diverses régions du Québec, le concept de fédération permet de faciliter la mise en place de services qui sont en mesure de pallier à ce problème. Les commissions scolaires et les cégeps de plus petites envergures pourraient, entre autres, profiter des meilleures pratiques, de méthodes, de l'infrastructure et de l'expertise dans différents domaines des organismes de plus grande envergure. Ce partage peut se faire sans menaces aux données plus sensibles de l'une ou l'autre des organisations éducatives grâce aux divers niveaux d'assurances définis par le NIST (*National Institute of Standards and Technology*).

Réflexion éthique

Les agences gouvernementales qui effectuent la collecte des informations concernant l'identité des citoyens doivent s'attendre à justifier ces collectes et l'utilisation de ces informations.

La réflexion éthique dans le domaine des technologies de l'information est vaste. En considérant les droits essentiels suivants :

- Le principe de même discrimination;
- Le droit à une prise en charge, à un accompagnement adapté;
- Le droit à l'information;
- Le principe du libre choix, du consentement éclairé et de la participation de sa personne;
- Le droit à la renonciation (dire non);
- Le droit aux respects des droits familiaux;
- Le droit à la protection;
- Le droit à l'autonomie;
- Principe du soutien;
- Droit à l'exercice des droits civiques;
- Droit à une participation religieuse;
- Droit au respect, à la dignité et à l'intimité.

Une fédération dans le domaine de l'éducation doit être en mesure de protéger ces droits sociaux en plus des lois auxquelles elle est assujettie. Dans le contexte de l'apprentissage en ligne, nous devons en premier lieu examiner toutes les exigences et mettre en évidence les risques associés aux menaces typiques. Le tableau suivant présente un exemple d'exigence et du risque associé potentiel.

Exigence (qualité)	Remarques	Risques
Disponibilité	Lors de l'apprentissage, la disponibilité n'est pas aussi importante que, par exemple, pendant les examens en ligne. Un temps d'arrêt de quelques heures est probablement acceptable pour les serveurs de contenu, mais manifestement pas pour les serveurs	Attaques du type « *Denial of service* » Le type d'attaque est différent pendant la période d'examen. Par exemple, un étudiant qui aimerait obtenir une seconde chance pourrait initier une attaque non seulement sur le serveur, mais sur les PC dans la classe…

	examen.	

Démarche

Plusieurs fédérations qui opèrent actuellement dans le domaine de l'enseignement ont été créées dans le cadre d'un projet national avec un objectif de fournir à tous les citoyens une identité numérique. C'est le cas du Royaume-Uni, du Danemark et de plusieurs autres pays. Bien sûr, nous avons aussi observé que les fédérations visant les études supérieures semblent inclure que la population universitaire a des besoins spécifiques par rapport à la population en général.

Un projet de l'envergure d'une fédération dans le domaine de l'enseignement au Québec implique plusieurs politiques générales et procédures devant être appliquées et entretenues. Voici une liste, déduite à partir de la littérature et nos observations sur plusieurs fédérations, qui présente quelques exemples :

- Certification — évaluation technique du réseau en fonction des exigences de sécurité;
- Chaîne d'accords de partenariat de confiance — un accord entre le partage d'informations des partenaires;
- Plan d'urgence — un plan pour maintenir la continuité des opérations;
- Mécanisme formel de traitement des dossiers — une politique de traitement des données;
- Contrôle d'accès de l'information — une politique pour différents niveaux d'accès à l'information;
- L'audit interne — l'inspection régulière des modèles d'accès;
- La sécurité du personnel — une politique de sécurité du personnel;
- Sécurité de gestion de configuration — une politique de coordination de la sécurité globale;
- Procédures d'incident de sécurité — une politique pour répondre aux incidents de sécurité;
- Processus de gestion de la sécurité — une politique pour gérer les failles de sécurité;
- Procédures de résiliation — une politique pour empêcher l'accès continu;
- Formation — sensibilisation à la sécurité pour le personnel.

Nous croyons que le ministère de l'Éducation doit donner son support politique et assurer la direction dans un tel dossier. Toutes les fédérations d'envergures se sont vues obtenir un tel support.

Enjeux

L'introduction d'une fédération amène, des processus distribués d'authentification et d'autorisation, ainsi que plusieurs requis au niveau de l'assurance (*LoA level of assurance*) selon une étude commandée par JISC (*The Joint Information Systems Committee*) au Royaume-Uni. L'étude vise à évaluer et à définir les concepts gravitant autour du niveau d'assurance dans une perspective nationale et internationale. Deux sondages, une version abrégée et une version longue ont été conduits auprès des usagers potentiels de la fédération ainsi que parmi les fournisseurs d'identités et de services. Trente organisations ont participé à l'étude parmi lesquelles on compte 24 éditeurs et quatre fédérations européennes des pays suivants : Norvège, Finlande, Danemark et Suisse.

Les niveaux d'assurance définis par le NIST permettent, suite à une analyse des risques et à la cartographie des risques identifiés, de choisir la technologie nécessaire pour atteindre les spécifications minimums d'un niveau correspondant à un risque. Le tableau « Requis techniques des niveaux d'assurance du NIST », en annexe, résume brièvement les quatre niveaux d'assurance du NIST.

Le niveau de confiance exigé dépend de la gravité des conséquences et de la probabilité de l'occurrence d'une mauvaise authentification. L'autorité américaine NIST (*National Institute of Standards and Technology*) définit quatre niveaux d'assurance. Ces niveaux requièrent des exigences pour :

- Les jetons;
- La validation, l'enregistrement et l'émission des titres de compétences en lien avec un jeton;
- La définition et l'utilisation de mécanisme d'authentification à distance;
- La définition de mécanismes d'assertions utilisés pour la communication des résultats d'une authentification à distance.

IL y a aussi les initiatives de diverses organisations gouvernementales et industrielles pour mettre en place des mécanismes, afin d'assurer un niveau d'assurance pour l'authentification.

Les catégories recensées de risques dans les sondages sont analogues pour les gouvernements du Royaume-Uni, des États-Unis et de l'Australie :

- Pertes financières;
- Préjudices à la réputation;
- Sécurité des personnes;
- Divulgation des renseignements personnels ou commerciaux sensibles à des tiers;
- Désagréments;

- Détresse causée à un tiers;

- Menaces à l’intégrité des systèmes des agences gouvernementales ou à leur capacité à la conduite des affaires courantes;

- Nuisance à la prévention du crime ou entrave à sa détection.

Étapes sommaires de mise en place

Le Québec, à ce jour, possède un parc informatique intéressant. Un grand nombre de citoyens ont accès à l'Internet à la maison et utilisent des services fournis par des compagnies privées ou par des organismes gouvernementaux. Dans le milieu de l'éducation, les organisations possèdent un réseau dans lequel les employés, les professeurs ou enseignants et les élèves ou étudiants ont une identité numérique. Toutefois, cette identité numérique ne peut pas, dans la plupart des cas, franchir le domaine de l'organisme. Ainsi, pour permettre de répandre les identités entre les divers organismes et au-delà, il faut créer une identité numérique fédérée.

Plusieurs perspectives doivent être adressées simultanément pour arriver à mettre en place une bonne stratégie de gestion de l'identité numérique. Il faut permettre le partage d'informations, de nouvelles idées, de nouvelles technologies et de bonnes pratiques dans le domaine de la gestion de l'identité. Le ministère de l'Éducation est l'acteur clé pour une telle entreprise. Il doit mettre en place les mécanismes permettant de créer la gouvernance décrite auparavant.

Lors de l'exploration de diverses fédérations existantes dans plusieurs pays, nous observons qu'un tel projet n'est pas un simple projet informatique. Une fédération dépasse les limites d'une simple organisation ou d'une entreprise. Voici les facteurs de succès que nous avons recensés dans la littérature :

- Équipement adéquat :
    - Investissement initial avant la réalisation de la fédération,
    - Vitesse des accès Internet des divers intervenants,
    - Infrastructures actuelles;
- Démonstration de comment une technologie répond aux besoins;
- Implication d'équipes de travail multidisciplinaires;
- Stratégies afin de s'assurer que les activités s'alignent pour un but commun :
    - Communication efficace entre les diverses parties prenantes;
    - Vision partagée à tous les niveaux de gouvernance;
    - Collaboration des divers participants dans la conception et sa gestion;
- Éditeurs et concepteurs de matériels pédagogiques doivent être informés du système mis en place;
- Création d'opportunités d'affaires pour les divers milieux;

- Utilisation de logiciel libre afin de permettre aux diverses parties prenantes de participer au développement;

- Objectifs réalistes avec des échéanciers réalisables;

- Cartographie des risques et des niveaux d'assurances nécessaires pour les services et les données impliquées dans l'authentification et l'autorisation;

- Identification des procédures d'enregistrement en accord avec les divers niveaux d'assurances lors de la création de la fédération et non lors de sa mise en application.

La fédération ne pourra pas progresser sans l'apport de tous les intervenants du milieu scolaire tant dans les domaines public que privé. La participation et le pragmatisme des parties prenantes ont eu un apport positif dans les fédérations du Danemark et du Royaume-Uni.

Conclusion

Nous estimons que le milieu de l'enseignement québécois doit s'engager éminemment dans la voie d'une identité numérique fédérée avec une meilleure cohérence entre les silos des commissions scolaires, cégeps, universités, institutions privées et certains organismes privés qui jouent un rôle stratégique. Les expériences documentées et les démarches en cours, tel que celle de la Colombie-Britannique et de certains pays européens, nous permettent d'envisager cette démarche avec optimisme.

Nous avons constaté que la gestion de l'identité numérique fédérée est un sujet très actuel non seulement en éducation, mais dans nombre d'autres sphères d'activité. Une telle identité est nécessaire et permettrait de résoudre plusieurs problématiques économiques et sociales.

Références

1. San-Tsai Sun et al., « A billion keys, but few locks : the crisis of web single sign-on », dans Proceedings of the 2010 workshop on New security paradigms, NSPW '10 (New York, NY, USA: ACM, 2010), 61–72.

2. I Djordjevic et T Dimitrakos, « A note on the anatomy of federation », BT Technology Journal 23, no. 4 (2005) : 89-106.

3. Wei Jie et al., « A Review of Grid Authentication and Authorization Technologies and Support for Federated Access Control. », ACM Computing Surveys 43, no. 2 (janvier 2011) : 12:1-12:26.

4. Miyata Teruko et al., « A Survey on Identity Management Protocols and Standards », IEICE Trans Inf Syst (Inst Electron Inf Commun Eng) E89-D, no. 1 (2006) : 112-123.

5. « Advanced Security for Virtual Organizations: The Pros and Cons of Centralized vs Decentralized Security Models » (mai 19, 2008) : 106-113.

6. Jean-Baptiste Lézoray, Marc Pasquet, « Enabling collaboration between heterogeneous circles of trust through innovative identity solutions » IEEE (mai 18, 2009) : 476-484.

7. Ashraf M. Abusharekh, Lawrence E. Gloss, et Alexander H. Levis, « Evaluation of Service Oriented Architecture-based federated architectures », Systems Engineering 14, no. 1 (2011) : 56-72.

8. Skratt, « From the Newsstand », IEEE Internet Computing 9, no. 6 (2005) : 10-13.

9. G. Peterson, « Introduction to identity management risk metrics », IEEE Security & Privacy Magazine 4, no. 4 (2006) : 88-91.

10. Joshua B. Bolten, « M-04-04 Memoramdum to the heads of all departements and agencies Subject : E-Authentification guidance for Federal Agencies » (Executive office of the president, décembre 16, 2003).

11. William E. Burr, Donna F. Dodson, et W. Timothy Polk, « NIST Special Publication, 800-63, Electronic Authentification Guideline » (National Institute of Standards and Technology, avril 2006).

12. Min Li et al., « Privacy-aware access control with trust management in web service », World Wide Web 14, no. 4 (2011) : 407-430.

13. [ISO 10181-3] Security Frameworks for Open Systems : Access Control Framework, ITU-T

14. [ISO X.509 9594-8] Information Technology - Open Systems Interconnection The Directory: Authentication Framework, ITU-T

15. Gue, D. G. (2005). The HIPAA security rule (NPRM): Overview. The HIPAAdvisory.com, Phoenix Health Systems. Retrieved June 5, 2005, from http://www.hipaadvisory.com/regs/securityoverview.htm

16. Les plates formes virtuelles d'apprentissage en Europe : que nous apprennent les expériences du Danemark, du Royaume-Uni et de l'Espagne? Panorama comparatif http://projets-ent.com/wp-content/uploads/2010/11/Benchmark_european-apprentissage.pdf

ANNEXE : Les perspectives multidimensionnelles de la gestion d'identité pour un fournisseur

Le tableau qui suit permet de visualiser et d'apprécier le volume d'informations qui doit être traité afin d'atteindre simultanément des objectifs de confidentialité, de niveau d'assurance et des assertions concernant l'identité.

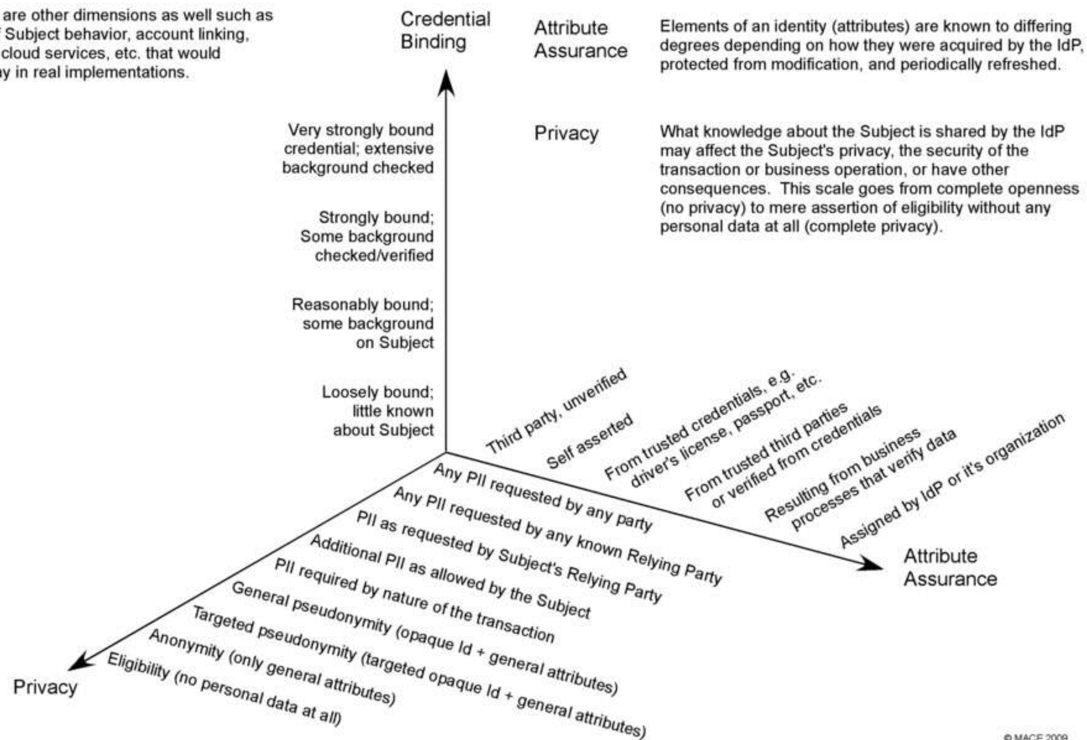


Image extraite du site : http://middleware.internet2.edu/tao-of-attributes/gfx/0_Identity_Axes.jpg créé par Internet2, qui est un consortium dirigé par *U.S. research and education community*.

Publications du GTN-Québec

2012-03	*Soutien au développement de ressources numériques pour l'enseignement et l'apprentissage dans les universités québécoises – Rapport complet.* Rédigé par Line Cormier, Maureen Clapperton, Nicolas Gagnon, Michel Gendron, Robert Gérin-Lajoie et Jean Marcoux, 71 p.
2012-02	*Soutien au développement de ressources numériques pour l'enseignement et l'apprentissage dans les universités québécoises – Les faits saillants.* Rédigé par Line Cormier, Maureen Clapperton, Nicolas Gagnon, Michel Gendron, Robert Gérin-Lajoie et Jean Marcoux, 10 p.
2012-01	*Manuels de cours numériques – droit d'auteur et gestion, inventaire des solutions disponibles version 1.1.* Rédigé par Réjean Payette, 38 p.
2011-06	*Les tableaux numériques interactifs : considérations d'interopérabilité.* Rédigé par Marc-Antoine Parent, 28 p.
2011-05	*Fédération d'identité pour les organismes de l'éducation.* Rédigé par André Breton, 50 p.
2011-04	*Compte-rendu de participation, 26ème colloque annuel CSUN 2011.* Rédigé par Denis Boudreau, 14 p.
2011-03	*Les environnements d'apprentissage sont-ils en mutation ou en gestation?* Rédigé par Pierre-Julien Guay, Marcel Borduas, Yves Otis, Robet Paré et Sacha Leprêtre, 21 p.
2011-02	*Profil d'application québécois de métadonnées pour les opportunités d'étude, d'apprentissage et de formation (v.0.7.5)* Rédigé par Gilles Gauthier, 93 p.
2011-01	*Profil d'application Normetic 2.0 (v0.7.5)* Rédigé par Gilles Gauthier, 41 p.
2010-01	*Évaluation de fonctionnalités de traitement des métadonnées par Alfesco en comparaison avec Normetic.* Rédigé par François Vincent, 9 p.
2009-06	*Portrait des pratiques de sélection, de catalogage et de partage des documents numériques dans les bibliothèques.* Rédigé par Marie-Chantal Dufour, 48 p.
2009-05	*Accès aux contenus de formation en ligne : difficultés des apprenants handicapés et solutions pour assurer l'accessibilité des contenus.* Rédigé par Denis Boudreau, 21 p.
2009-04	*Développement MLO: Metadata for learning opportunities.* Rédigé par Olivier Gerbé et Thi-Lan-Anh Dinh, 32 p.
2009-03	*Concept and Prototype of an Aggregator Portal for Learning Opportunities Based on the MLO-AD Standard.* Rédigé par Katharina Bauer-Öppinger, 89 p.

(autres publications à la quatrième de couverture)

Publications du GTN-Québec (suite)

2009-02	*Identification des caractéristiques des modèles de diffusion de contenus numériques : recension des dépôts numériques existants – Partie 2.* Rédigé par Gabriel Dumouchel et Thierry Karsenti, 99 p.
2009-01	*Identification des caractéristiques des modèles de diffusion de contenus numériques : revue de littérature – Partie 1.* Rédigé par Gabriel Dumouchel et Thierry Karsenti, 54 p.
2008-05	*Ressources d'apprentissage et normes : la situation au Québec.* Rédigé par Christian Lafrance, 102 p.
2008-04	*Guide d'élaboration de fiches descriptives de ressources d'enseignement et d'apprentissage selon Normetic v1.2, profil d'application québécois du standard Learning Object Metadata (LOM).* Rédigé par Gérald Roberge, 57 p.
2008-03	*Profil d'application Normetic 1.2*. Rédigé par Gérald Roberge, 170 p.
2008-02	*Tableau du code XML à produire pour le vocabulaire de l'élément 5.2 de Normetic 1.2*. Rédigé par Gérald Roberge
2008-01	*Tableau du code XML à produire pour le vocabulaire de l'élément 5.6 de Normetic 1.2.* . Rédigé par Gérald Roberge
2007-01	*Portrait général des stratégies d'assurance qualité des ressources d'enseignement et d'apprentissage (REA) : à l'attention des gestionnaires.* Rédigé par Karin Lundgre-Cayrol, Suzanne Lapointe et Ileana De la Teja, 25 p.
2006-03	*Les normes, comment?* Rédigé par Gérald Roberge, 4 p.
2006-02	*Les normes, pourquoi?* Rédigé par Gérald Roberge, 4p.
2006-01	*Guide pour la sélection de REA.* Rédigé par Gérald Roberge, 10 p.
2005-01	*Le profil d'application Normetic, version 1.1.* Rédigé par Robert Thivierge, 8 p.
2003-01	*La description normalisée des ressources : vers un patrimoine éducatif – Normetic, version 1.0.* Sous la supervision de la CREPUQ et Novasys inc., 139 p.
2002-01	*Les normes et standards de la formation en ligne – État des lieux et enjeux.* Rédigé par Rachel Chouinard. Sous la supervision de la CREPUQ et du sous-comité SCTIC, 39 p.

Pour télécharger ces publications ou pour la liste complète des publications du GTN-Québec, voir le site Web **www.gtn-quebec.org/publications**